AF/IFW

Docket 81399NAB
Customer No. 01333

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of

Babak Tehranchi

AN ENCRYPTION APPARATUS AND METHOD FOR SYNCHRONIZING MULTIPLE ENCRYPTION KEYS WITH A DATA STREAM

Serial No. 09/656,634

Filed September 07, 2000

Group Art Unit: 2132

Examiner: Lanier, Benjamin E.

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Tara Piccone
Tara Piccone

1-20-06
Date

Mail Stop APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Sir:

APPEAL BRIEF TRANSMITTAL

Enclosed herewith is Appellants' Appeal Brief for the above-identified application.

The Commissioner is hereby authorized to charge the Appeal Brief filing fee to Eastman Kodak Company Deposit Account 05-0225. A duplicate copy of this letter is enclosed.

Respectfully submitted,

Attorney for Appellants
Registration No. 29,134

Nelson A. Blish/tmp
Telephone: 585-588-2720
Facsimile: 585-477-4646
Enclosures

If the Examiner is unable to reach the Applicant(s) Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.

Docket 81399NAB
Customer No. 01333

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of

Babak Tehranchi

AN ENCRYPTION APPARATUS
AND METHOD FOR
SYNCHRONIZING MULTIPLE
ENCRYPTION KEYS
WITH A DATA STREAM

Serial No. 09/656,634

Filed 07 September 2000

Group Art Unit: 2132

Examiner: Lanier, Benjamin E.

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Tara Piccone
Tara Piccone

1-20-06
Date

Mail Stop APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Sir:

APPEAL BRIEF PURSUANT TO 37 C.F.R. 41.37 and 35 U.S.C. 134

Table Of Contents

APPELLANT'S BRIEF ON APPEAL

Appellant hereby appeals to the Board of Patent Appeals and Interferences from the Examiner's Final Rejection of claims 1-3, 5-47, 50-58, and 62-77 which was contained in the Office Action mailed August 29, 2005.

A timely Notice of Appeal was filed on November 22, 2005.

Real Party In Interest

The assignee, Eastman Kodak Company, is the real party in interest.

Related Appeals And Interferences

No appeals or interferences are known which will directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

Status Of The Claims

Claims 1-3, 5-47, 50-58, and 62-77 are pending in the application.

Claims 4, 48, 49, and 59-61 have been canceled.

Claim 3 stands finally rejected under 35 U.S.C. 112, paragraph 2.

Claim 47 stands finally rejected under 35 U.S.C. 112, paragraph 1.

Claims 62-71 stand finally rejected under 35 U.S.C. 101.

Claims 28, 30, 32-36, 38-41, 43, 44, 52, 58, 62-69, and 73 stand finally rejected under 35 U.S.C. 102.

Claims 1-3, 5-16, 18-27, 31, 37, 42, 45-47, 50, 53-57, 58, 70-72, 74, 75, and 76 stand finally rejected under 35 U.S.C. 103.

All the final rejections of Claims 1-3, 5-47, 50-58, and 62-77 are the subjects of this appeal.

Appendix I provides a clean, double spaced copy of the claims on appeal.

Status Of Amendments

A Notice of Appeal was filed on November 22, 2005. No amendments have been filed after the final rejection.

Summary of Claimed Subject Matter

With particular reference to specification page 10 line 30- page 11 and 12, independent Claim 1 is directed to a data transfer apparatus (see Figure 1 item 10) for the secure transfer from a digital data source (18, 12) to a digital data receiver (14) of a plurality of data blocks. Each data block (Figure 2 item 26) comprises plural frames of a digital video image. The apparatus comprises an encryption key generator (Figure 1 item 28) for providing encryption keys wherein a respective encryption key is assigned to each data block of the plurality of data blocks. A block synchronization index (specification page 11-page 12) is provided indicating a correspondence between the encryption key and the data block. An encryption engine (22) produces an encrypted data block using the encryption key from the encryption key generator. A data transmission channel (32) delivers the encrypted data block from the encryption engine to the digital data receiver (14). A key transmission channel (34) delivers the encryption key from the encryption key generator to the digital data receiver. A block synchronization channel (78) delivers the block synchronization index from the encryption key generator to the digital data receiver. A memory (specification page 21 line 24-line 6) stores the encryption keys at the digital data receiver and the digital data receiver includes a decryption engine (38) that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block.

With particular reference to specification page 20 and Figure 7, Claim 20 is an independent claim directed to a method for the secure transfer of a data stream from a digital source to a digital data receiver. The method comprises the steps of partitioning the data stream into a plurality of successive data blocks wherein the size of each successive data block is variable (specification page 20 lines 8-9) based on an average size (specification page 20 lines 17-18) and based on a randomly generated offset (line 10 item 76) . For each successive data block an encryption key is generated. Each data block is encrypted using the encryption key to provide an encrypted data block. Furthermore, the method includes the step of generating a synchronization index associating the encrypted data block with the encryption key.

With particular reference to specification page 10 starting line 30, page 11 and 12, Claim 28 is directed to a method for the secure transfer of a digital motion image data stream from a digital data source to a digital data receiver. The method of claim 28 includes the steps of partitioning a digital motion image data stream into a plurality of digital motion image data blocks, generating a plurality of encryption keys and generating an encrypted digital motion image data stream by repetition of various recited steps for each of the plurality of digital motion image data blocks. The steps include encrypting each digital motion image data block using a distinct encryption key to create an encrypted video data block. The encrypted data block is stored as part of an encrypted digital motion image data stream. A synchronization index is generated that associates each digital motion image data block with each distinct encryption key. Providing the encrypted digital motion image data stream to the digital data receiver (14). A synchronization_index is provided to the digital data receiver. The encryption keys are stored at the digital data receiver in a memory (see for example specification page 21 line 24-page 22 line 6), and the digital data receiver includes a decryption engine (38) that is responsive to the synchronization index and the decryption engine mapping each key into memory to a respective encrypted data block for use in decryption of the respective data block.

With particular reference to specification page 14 line 14-page 15 line 22, Claim 36 is an independent claim directed to a method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion image. The method of claim 36 includes the steps of providing a plurality of encryption keys separately from encrypted data blocks and storing the encryption keys into memory (specification page 21 line 24-page 22 line 6) at a digital data receiver (14). An identifier is provided that correlates a mapping algorithm to the plurality of encryption keys and a decryption engine (38) is operated that is responsive to the identifier in the mapping algorithm to generate each key for use in decryption of the respective data block.

With particular reference to Claim 47 is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method includes providing digital motion image data as digital motion image data blocks at least some of which digital motion image data blocks are different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks. In response to an index that provides information identifying a first frame of each digital motion image data block there is generated a corresponding key from a plurality of encryption keys for use in decrypting the respective digital motion image data blocks. At least some of the digital motion image data blocks each represent plural frames of the motion picture.

With reference to specification page 33 and original Claim 52, present Claim 52 is an independent claim directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method comprises providing digital motion image data blocks that are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames and wherein the P and B frames are encrypted. The method further comprises generating a corresponding key from the plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted.

With reference to specification page 33 and original Claim 53, present Claim 53 is an independent claim directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The steps of this claim comprise providing digital motion image data of a digital motion picture as digital motion image data blocks. The digital motion image data frame comprises plural color components and only data of one of the color components is encrypted. The method of Claim 53 provides for reduced image processing in that only one of the color components is encrypted.

With reference to specification page 16 lines 3-18 and to Figure 5, independent Claim 62 is a claim directed to a data structure for use in providing an encryption key. The data structure comprises a component ID field (56, 58) that has plural bits mapping information for identifying an image frame of an image block in which a specific encryption key is first used. The image block is composed of plural image frames. An encryption key field (60) of plural bits forms the encryption key and is operative for use in decrypting the image block.

With reference to specification page 21 line 24-page 22 line 6 and Figure 6, Claim 66 is an independent claim directed to a data structure providing a key field (68) comprising a plurality of respective keys for decryption of respective blocks of frames of a motion picture. The data structure comprises a synchronization field (64) containing synchronization index information operative to link individual keys to respective blocks of video image data. Each block comprises plural frames of the motion picture. A key field represents plural encryption keys that are operative for use in decryption of the respective image frames.

With reference to specification page 19 line 25-page 22 line 6 and Figure 6, Claim 72 is an independent claim directed to a method of decryption of a motion picture having a plurality of image frames. The method comprises the steps of providing a plurality of encrypted video image blocks which in combination comprise the motion picture in encrypted form. The encrypted video image blocks each represent information of a plurality of image frames of the motion picture. Each image frame begins at a frame beginning and at least some of the image blocks are sized to encrypt different numbers of image frames. A synchronization field is provided. A key field is provided and comprises a plurality of keys. Each key is suited for decryption of a respective image block. The decryption engine uses the synchronization field and the keys in the key field to create a table or matrix in the memory that maps each key to its respective image block.

With reference to specification page 19 line 25-page 22 line 6 and Figure 6, Claim 73 is an independent claim directed to in a method for the decryption of an individual image frame of an encrypted motion picture, a method of generating a key for use in decryption of the individual image frame. In this key generating method there is provided an identification of an image frame to be decrypted. There is provided a synchronization index to map a plurality of encryption keys, keys being suited for use in decrypting respective blocks of image data forming a motion picture. In response to the identification of the image frame and the synchronization index outputting a corresponding key for decrypting of the specific image frame.

Grounds of Rejection to be Reviewed on Appeal

The following issues are presented for review by the Board of Patent Appeals and Interferences. Unless indicated otherwise in the Arguments section of this BRIEF, all claims are submitted to be separately patentable from any other claim and the patentability thereof will be separately argued in the Arguments section.

1. Is claim 3 definite under 35 USC 112, paragraph 2?

2. Does claim 47 comply with the written description requirement of 35 USC 112, paragraph 1?

3. Are claims 62-71 directed to statutory subject matter as defined in 35 USC 101?

4. Are claims 28, 30, 32-36, 38-41, 43, 44, 52, 58, 62-69, 73 and 77 unpatentable as being anticipated by Warren et al., US patent 5,963,909, (hereinafter referred to as Warren) under 35 USC 102?

5. Are claims 12, 18 and 31 unpatentable as being obvious in view of Warren under 35 USC 103?

6. Are claims 1-3, 5-10, 13, 15, 16, 17, 20-25, 27, 47, 52, 57, 58, 72, 74 and 75 unpatentable as being obvious in view of Warren taken with Rump et al. , US patent 6,735,311, (hereinafter referred to as Rump) under 35 USC 103?

7. Are claims 11, 14 unpatentable as being obvious in view of Warren taken with Handelman et al., US patent 5,774,546, (hereinafter referred to as Handelman) under 35 USC 103?

8. Is claim 19 unpatentable as being obvious in view of Warren taken with the Schneier reference, Applied Cryptography, second edition, pages 372-373, under 35 USC 103?

9. Are claims 26, 37 unpatentable as being obvious in view of Warren taken with Dahan et al., US patent 6,137,763, (hereinafter referred to as Dahan) under 35 USC 103?

10. Are claims 42, 45, 46, 50, 53-56 and 76 unpatentable as being obvious in view of Warren taken with Chaum, US patent 5,959,717, under 35 USC 103?

11. Are claims 70, 71 unpatentable as being obvious in view of Warren taken with Rabowsky, US patent 6,141,530, under 35 USC 103?

12. Are claims 29 and 51 patentable over the prior art? (Note that the final rejection mentions these two claims as being rejected only in the summary and not in the body of the final rejection)

Arguments

1. Claim 3 is definite under 35 USC 112, paragraph 2. Claim 3 stands finally rejected under 35 USC 112, paragraph 2, as being indefinite. The Examiner notes

that there is insufficient antecedent basis for use of the term"said single data block." It is submitted that the claim itself is clear in that it refers to a data block and one of ordinary skill in the art would consider said single data block to be referring to such date block. Therefore, it is respectfully submitted that the claim is definite and not per se objectionable under the reasonableness test of 35 USC 112.

2. Claim 47 complies with the written description requirement of 35 USC 112, paragraph 1. The Examiner objects to the inclusion by amendment to claim 47 of the term "digital motion image data blocks at least some of which digital motion image data blocks are different sizes to provide at least some variability." No explanation is provided by the Examiner as to why description on pages 20-21 does not support claim 47 as amended. As may be noted in the specification, page 20 starting at line 7, "using blocks 26 of the same size is a simple approach, but a more secure solution is to introduce some randomness and sizing blocks 26." The description in the specification makes reference to Figure 7 noting that this figure shows that frames of motion picture data will have different offsets (or start positions). The description following on pages 20-21 provides an explanation of how the block boundaries are determined at various points so that the different motion picture data blocks contain a random number of frames. As the data blocks are of different sizes they thus inherently produce some variability in terms of the number of frames of the motion picture in the data blocks. It is submitted that this description satisfies the written description requirement of 35 USC 112, first paragraph, with regard to the term found objectionable by the Examiner. Even though the specification as originally filed may not have exact duplication in the wording now found in claim 47 as amended such exact duplication is not required and it is submitted that the specification as originally filed provides sufficient support for the subject matter of present claim 47.

3. Claims 62-71 are directed to statutory subject matter as defined in 35 USC 101. In considering the patentability of claims 62-71 under 35 USC 101 any representative claim may be used.

Claims 62-71 are rejected by the Examiner as being non-statutory for the reason that they claim a data structure alone "which is not limited to the technological arts." As noted in In re Oetiker "The examiner bears the initial burden...of presenting a prima facie case of unpatentability." In re Oetiker, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In evaluating whether a claim meets the requirements of section 101, the Supreme Court requires that the claim be considered as a whole to determine whether it is for a particular application of an abstract idea rather than for the abstract idea itself. The Supreme has quite broadly stated that "Congress intended statutory subject matter to 'include anything under the sun that is made by man.'" Diehr, 450 U.S. at 182, 209 USPQ at 6. Furthermore as clearly indicated in Annex III of the USPTO's Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility published 22 Nov 2005:

> "United States patent law does not support the application of a "technical aspect" or "technological arts" requirement. Title 35 of the United States Code does not recite, explicitly or implicitly, that inventions must be within the "technological arts" to be patentable."

Thus, the Examiner is using a discredited reason for rejecting Claims 62-71 under 35 USC 101. Applicant is aware of In re Warmerdam, 31 USPQ 2nd 1754 (Fed. Cir. 1994). However, it is respectfully submitted that no per se rule was authorized in this case and that analysis of the claims as a whole is required by the Examiner. Furthermore, claim 62 refers to a data structure that includes a component ID field having plural bits mapping information for identifying an image frame of an image block. Bits represent basic information for a computer and are tangible. It is submitted that this is sufficient tangible structure to support the requirements of 35 USC 101.

4. Claims 28, 30, 32-36, 38-41, 43, 44, 52, 58, 62-69, 73 and 77 are not unpatentable as being anticipated by Warren under 35 USC 102. Unless otherwise indicated the claims are separately patentable.

At the outset it should be recognized that anticipation under 35 USC 102 requires that each element of the claim under consideration be taught by the reference.

Claim 28 is directed to a method for the secure transfer of a digital motion image data stream from a digital data source to a digital data receiver. The method of claim 28 includes the steps of partitioning a digital motion image data stream into a plurality of digital motion image data blocks, generating a plurality of encryption keys and generating an encrypted digital motion image data stream by repetition of various recited steps for each of the plurality of digital motion image data blocks. The steps include encrypting each digital motion image data block using a distinct encryption key to create an encrypted video data block. The encrypted data block is stored as part of an encrypted digital motion image data stream. A synchronization index is generated that associates each digital motion image data block with each distinct encryption key. Providing the encrypted digital motion image data stream to the digital data receiver. A synchronization index is provided to the digital data receiver. The encryption keys are stored at the digital data receiver in a memory, and the digital data receiver includes a decryption engine that is responsive to the synchronization index and the decryption engine mapping each key into memory to a respective encrypted data block for use in decryption of the respective data block. As the Examiner notes Warren discloses a copy management system wherein data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block. In this regard the Examiner refers to Figure 13 of Warren. The Examiner further refers to Figure 12 of Warren wherein each data block contains an encryption key for the frame contained in the next data block. According to the Examiner this implies and "meets the limitation" of a block synchronization index indicating a correspondence between the encryption key and the single data block. The Examiner is thus apparently of the opinion that the encryption key of Warren is its own index. However, within the disclosure of Warren there is no indication that there is any generation of a synchronization index that associates each said digital motion image data block with each distinct encryption key. There is merely generation of an encryption key that is associated with an image data block. For this reason it is submitted that Claim 28 is not anticipated or even rendered obvious by Warren.

For purposes of this appeal only, the patentability of each of Claims 30, 32 and 33 stands or falls with that of Claim 28. These claims are dependent claims of Claim 28.

Claim 34 is a dependent claim of claim 28 and recites that the step of providing the synchronization index to the digital data receiver comprises the step of transmitting the synchronization index. As there is no indication in Warren of a synchronization index there is also know no teaching or even suggestion by Warren that would anticipate a claim such as Claim 34 that recites the step of transmitting the synchronization index. For this reason it is submitted that Claim 34 is not anticipated or even rendered obvious by Warren.

Claim 35 is a dependent claim of Claim 28 and adds that wherein the step of providing said synchronization index to the digital data receiver comprises the step of recording the synchronization index onto a storage medium. The Examiner's sole comment with regard to this is that the encrypted data is recorded on a medium. However, there is no indication in Warren or suggestion of recording a synchronization index onto the storage medium wherein the synchronization index as set forth in Claim 28 is one that associates each digital motion image data block with each distinct encryption key. For this reason it is submitted that Claim 34 is not anticipated or rendered obvious by Warren.

Claim 36 is an independent claim directed to a method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion image. The method of claim 36 includes the steps of providing a plurality of encryption keys separately from encrypted data blocks and storing the encryption keys into memory at a digital data receiver. An identifier is provided that correlates a mapping algorithm to the plurality of encryption keys and a decryption engine is operated that is responsive to the identifier in the mapping algorithm to generate each key for use in decryption of the respective data block. In the final rejection the Examiner notes that each data block in Warren contains an encryption key for the frame contained in the next data block "which meets the limitation providing an identifier that correlates a mapping algorithm to said plurality of encryption keys." However, there is no indication of such an identifier that performs this function and the recited step. There is merely the presence of location of the key relative to the data block. There is no identifier that is disclosed that correlates a mapping algorithm to the plurality of encryption keys. For this reason it is submitted that Claim 36 is not anticipated or rendered obvious by Warren.

Claim 38 is a dependent claim of claim 36 and further comprises the step of padding the plurality of encryption keys using dummy bits. An advantage of this would be to make decryption of the keys by unauthorized persons more difficult since extra bits are used with each encryption key. Warren at column 14, lines 18-21 discloses that some keys may be null keys so that apparently these null keys can be used with unencrypted frames. The null keys are thus not associated with encrypted frames and thus do not comprise encryption keys that correspond to a plurality of encrypted data blocks. For this reason it is submitted that Claim 38 is also not anticipated or rendered obvious by Warren.

Claim 39 is a dependent claim of claim 36 and further comprises the step of providing a digital motion image data frame or frame component identification and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part. In Warren there is no step of providing a frame or frame component identification that is then used to generate a corresponding key from the plurality of encryption keys for use in decrypting the pertinent data block. There is merely location of corresponding keys with corresponding data blocks but no teaching of generating a corresponding key from the plurality of encryption keys using a frame or frame component identification. For this reason it is submitted that Claim 39 is not anticipated or rendered obvious by Warren.

Claims 40, 41, 43 and 44 are dependent claims of claim 39. For purposes of this appeal only, the patentability of Claims 40, 41, 43 and 44 stand and fall with that of Claim 39.

Claim 52 is an independent claim directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method comprises providing digital motion image data blocks that are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames and wherein the P and B frames are encrypted. The method further comprises generating a corresponding key from the plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted. There are no specific comments by the Examiner with regard to anticipation of Claim 52. Although there may be disclosure in Warren of MPEG type compression there is no indication in Warren of a step of having the P and B frames be encrypted and generating a corresponding key from the plurality of encryption keys for use in decrypting the image data block that is encrypted. For this reason it is submitted that Claim 52 is not anticipated or rendered obvious by Warren.

Claim 58 is a dependent claim of independent Claim 47. As claim 47 is not the subject of an anticipation rejection under Warren it would appear to be in error to have Claim 58 be the subject of an anticipation rejection. Claims 47 and 58 are rejected for obviousness in view of Warren taken with Rump. Dependent claim 58 is directed to a method of decrypting encrypted digital motion picture image data blocks that includes the steps of providing digital motion image data blocks that are of different sizes to provide at least some variability in terms of numbers of frames of a motion picture in the image data blocks. In response to an index providing information identifying a first frame of each digital motion image data block a corresponding key is generated from a plurality of encryption keys for use in decrypting the respective digital motion image data block. Claim 58 further includes the feature of having indices providing correspondence information relative to encryption keys in a channel separate from a channel providing cipher text of the encrypted data blocks. There is no indication in Warren of providing digital motion image data blocks that are of different sizes to provide at least some variability in terms of numbers of frames of the motion picture in the image data blocks. For this reason it is submitted that Claim 58 is not anticipated or rendered obvious by Warren.

Claim 62 is a claim directed to a data structure for use in providing an encryption key. The data structure comprises a component ID field that has plural bits mapping information for identifying an image frame of an image block in which a specific encryption key is first used. The image block is composed of plural image frames. An encryption key field of plural bits forms the encryption key and is operative for use in decrypting the image block. In Warren each key is associated with a single image frame. There is no disclosure in Warren of a field that has plural bits mapping information for identifying an image frame of an image block in which a specific encryption key is first used. The reason for this is that there is no need for such a field in Warren because there is correspondence between an encryption key and its respective frame or frames through placement on the storage medium. For this reason it is submitted that Claim 62 is not anticipated or rendered obvious by Warren.

Claim 63 is a dependent claim of Claim 62 and adds the feature that a start component ID field of plural bits is operative to identify the start of the data structure. There is no disclosure in Warren of this feature as well as Warren does not identify the structure of the key field used by him. For this reason it is submitted that Claim 63 is not anticipated or rendered obvious by Warren.

Claim 64 is a dependent claim of Claim 63 and is directed to a composite data structure having plural component data structures as defined in Claim 63 for providing plural encryption keys. Each image block is composed of plural image frames and each component data structure comprises a component ID field having plural bits mapping information for an image frame of the image block in which a specific encryption key is first used. The component data structure further comprises an encryption key field of plural bits forming the encryption key that is operative for use in the decryption of the image block. As noted above there is no teaching nor suggestion and even need for such a field in Warren because there is an encryption key for a frame or frames that are located on a storage medium in relative correspondence. For this reason it is submitted that Claim 64 is not anticipated or rendered obvious by Warren.

Claim 65 is a dependent claim of Claim 64 and adds the feature that the composite data structure includes a start component ID field of plural bits that is used to identify the start of the component data structure. There is no disclosure in Warren of this feature as well as Warren does not identify the structure of the key field used by him. For this reason it is submitted that Claim 65 is not anticipated or rendered obvious by Warren.

Claim 66 is an independent claim directed to a data structure providing a key field comprising a plurality of respective keys for decryption of respective blocks of frames of the motion picture. The data structure comprises a synchronization field containing synchronization index information operative to link individual keys to respective blocks of video image data. Each block comprises plural frames of the motion picture. A key field representing plural encryption keys that are operative for use in decryption of the respective image frames. As noted above Warren provides correspondence between a key and its respective image frame or frames through relative location or placement. There is no indication of a data structure providing a key field of respective keys with a synchronization field containing synchronization index information to link individual keys to respective blocks of video image data. For this reason it is submitted that Claim 66 is not anticipated or rendered obvious by Warren.

Claim 67 is a dependent claim of Claim 66 and adds the feature that the data structure includes a key overhead field having information indicating how keys are arranged in the key field. There is no description in Warren of a data structure that includes any information indicating how keys are arranged in the key field. As noted above Warren merrily describes keys that are arranged on a record member to be in order for the appropriate image frame or frames. For this reason it is submitted that Claim 67 is not anticipated or rendered obvious by Warren.

Claim 68 is a dependent claim of Claim 66 and is directed to the data structure that includes a key overhead field having information indicating how the blocks of video image data a structured. In Warren the video image data is structured one after the other on a recording member so that there is no information on any recording member indicating how the blocks of video image data are structured. For this reason it is submitted that Claim 68 is not anticipated or rendered obvious by Warren.

Claim 69 is a dependent claim of claim 66 and adds the feature that the data structure includes a key overhead field having information specifying an algorithm used to locate a corresponding key within the key field. There is no such equivalent data structure found in Warren. The Examiner appears to be implying that rigid structure or more precisely specific arrangement of keys and corresponding frames in Warren is an equivalent of information that is part of the data structure as claimed by applicant. Such arrangement only represents what is and does not represent or comprise information representing a key overhead field as claimed by applicant. For this reason it is submitted that Claim 69 is not anticipated or rendered obvious by Warren.

Claim 73 is directed to in a method for the decryption of an individual image frame of an encrypted motion picture, a method of generating a key for use in decryption of the individual image frame. In this key generating method there is provided an identification of an image frame to be decrypted. There is provided a synchronization index to map a plurality of encryption keys, keys being suited for use in decrypting respective blocks of image data forming a motion picture. In response to the identification of the image frame and the synchronization index outputting a corresponding key for decrypting of the specific image frame. The Examiner refers to the embodiment of Warren Figure 17 wherein there is provided for the multiplexing of the various signals including image blocks and respective keys. As noted in the specification of Warren the keys are arranged in an orderly arrangement relative to the respective frames so that processing of the key signals and the respective frames by the multiplexer may occur. However, there is no description or teaching in Warren of a synchronization index that maps a plurality of encryption keys so that in response to the identification of the image frame and the synchronization index there is output of the corresponding key for decrypting of the specific image frame. For this reason it is submitted that Claim 73 is not anticipated or rendered obvious by Warren.

Claim 77 is a dependent claim of Claim 73. For purposes of this appeal only, the patentability of claim 77 stands or falls with that of Claim 73.

5. Claims 12, 18 and 31 are not unpatentable as being obvious in view of Warren under 35 USC 103. All of these claims are separately patentable.

Claim 12 is a dependent claim of Claim 1. Claim 1 is directed to a data transfer apparatus for the secure transfer of a plurality of data blocks wherein each data block comprises plural frames of the digital video image. The apparatus comprises an encryption key generator for providing encryption keys wherein a respective encryption key is assigned to each data block. A block synchronization index is provided indicating a correspondence between the encryption key and the data block. A memory stores the encryption keys at a digital data receiver and the digital data receiver includes a decryption engine that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block. Claim 12 further adds the feature of having the block synchronization index be encrypted. The Examiner is apparently of the opinion that it would be obvious to encrypt a synchronization index even though Warren does not disclose or suggest a synchronization index. The Examiner uses the possible teaching in Warren of relative position to be the equivalent of an index. However, no specific index is disclosed in Warren and therefore it is not seen how such could render obvious a claim combination reciting encryption of such an index. For this reason it is submitted that Claim 12 is not rendered obvious by Warren.

Claim 18 is also a dependent claim of Claim 1. Claim 1 is directed to a data transfer apparatus for the secure transfer of a plurality of data blocks wherein each data block comprises plural frames of a digital video image. The apparatus comprises an encryption key generator for providing encryption keys wherein a respective encryption key is assigned to each data block. A block synchronization index is provided indicating a correspondence between the encryption key and the data block. A memory stores the encryption keys at a digital data receiver and the digital data receiver includes a decryption engine that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block. Claim 18 further adds that the block synchronization index is computed using a pseudo-random number generator. According to the Examiner, Warren discloses that the system can use a number of different associations between the encryption keys and the data frames. However, the description of Warren assumes some orderly arrangement of encryption keys is provided so that there is a direct sequence between the encryption keys and the corresponding respective image frames. Thus, in Warren buffering can be used when there is a lack of timely simultaneous presentation of the encryption key and its corresponding image frame or frames. However, there is no disclosure or suggestion in Warren of a synchronization index and further no disclosure of a synchronization index that is computed using a pseudo-random number generator as called for by Claim 18. The Examiner merely provides a conclusion of obviousness without consideration of the lack of disclosure in Warren of even a synchronization index. For this reason it is submitted that Claim 18 is not rendered obvious by Warren.

Claim 31 is a dependent claim of Claim 28. Claim 28 is directed to a method for the secure transfer of digital motion image data streams from a digital data source to a digital data receiver. The method comprises positioning the digital motion image data streams into a plurality of digital motion image data blocks. A plurality of encryption keys is generated and a digital motion image data stream is encrypted by repetition of particularly set forth steps for each of the plurality of digital motion image data blocks. The steps include encrypting the digital motion image data block using a distinct encryption key and storing the thus encrypted data block as part of the digital motion image data stream. A synchronization index is generated that associates each digital motion image data block with each distinct encryption key. The encrypted digital motion image data streams are provided to the digital data receiver. The synchronization index is provided to the digital data receiver. The encryption keys are stored at the digital data receiver in a memory and the digital data receiver includes a decryption engine that is responsive to the synchronization index and the decryption engine maps each key in a memory to a respective encrypted data block for use in decryption of the respective data block. The method of claim 31 further recites that the step of generating a synchronization index further comprises encrypting said synchronization index. The Examiner acknowledges that Warren does not disclose "that this association is encrypted." However, it is noted that Warren does not even disclose a synchronization index. Warren does not disclose a digital data receiver that includes a decryption engine that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block. So it is submitted respectfully that Warren fails to render obvious the subject matter of Claim 31 for numerous reasons. For these reasons it is submitted that Claim 31 is not rendered obvious by Warren.

6. Claims 1-3, 5-10, 13, 15, 16, 17, 20-25, 27, 47, 52, 57, 58, 72, 74 and 75 are not unpatentable as being obvious in view of Warren taken with Rump under 35 USC 103. Unless otherwise indicated the claims are separately patentable.

Claim 1 is directed to a data transfer apparatus for the secure transfer from a digital data source to a digital data receiver of a plurality of data blocks. Each data block comprises plural frames of a digital video image. The apparatus comprises an encryption key generator for providing encryption keys wherein a respective encryption key is assigned to each data block of the plurality of data blocks. A block synchronization index is provided indicating a correspondence between the encryption key and the data block. An encryption engine produces an encrypted data block using the encryption key from the encryption key generator. The data transmission channel delivers the encrypted data block from the encryption engine to the digital data receiver. The key transmission channel delivers the encryption key from the encryption key generator to the digital data receiver. The block synchronization channel delivers the block synchronization index from the encryption key generator to the digital data receiver. A memory stores the encryption keys at the digital data receiver and the digital data receiver includes a decryption engine that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block. The Examiner's position with regard to Claim 1 is that Warren discloses that each block of data is encrypted with an encryption for that specific block which meets the limitation of an encryption key generator for providing an encryption key assigned to each single data block. However, even though the Warren reference does not disclose that the synchronization index is used to map each key in a memory to a respective encrypted data block, the Examiner responds with an interpretation of Warren as providing an inherent index because there is a relationship between the key stream and the data block. Thus, according to the Examiner, when the decryption unit stores the key stream to perform the decryption operation, the keys are somehow mapped in a memory, which is not disclosed, because "the key stream is ordered from the data block." However, there is no disclosure in Warren of a digital data receiver that is responsive to a synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block. The Examiner further identifies Rump as disclosing a system for encryption and decryption of multimedia data wherein each block contains a block size index which meets the limitation in certain of applicant's claims that the size of the digital data block may be different. In this regard, the Examiner is referring to Figure 2 of Rump wherein line 32 discloses that a block size index indicates the total amount of multimedia data which are assigned to the specific data block. However, it is not seen that this information is related to the number of frames within the data block or how one of ordinary skill in the art would be induced to combine the disclosure of Rump with that of Warren to obtain the subject matter of Claim 1. For this reason it is submitted that Claim 1 is not rendered obvious by the combination of Warren taken with Rump.

For purposes of this appeal only, the patentability of Claim 2 stands or falls with that of Claim 1.

Claim 3 is a dependent claim of Claim 1 and adds the feature that the size of the single data block is further conditioned by an offset value. The Examiner acknowledges that Warren does not disclose having different size data blocks identified by an offset value. Instead the Examiner refers to Rump (Figure 2, and column 7, line 18) wherein there is disclosed a block size index. This index disclosed by Rump is noted to be the total amount of multimedia data which is assigned to the specific data block however where there are plural data blocks there are provided several block size indexes. Thus it appears that this combination of references does not meet the requirement of Claim 3 of a data transfer apparatus that has data blocks such that each data block comprises plural frames of a digital video image, that an encryption key is assigned to each data block and a block synchronization index is provided indicating a correspondence between the encryption key and the data block. Furthermore, the size of the data block of Claim 3 is conditioned by an offset value. For this reason it is submitted that Claim 3 is not rendered obvious by the combination of Warren taken with Rump.

For purposes of this appeal only, the patentability of each of Claims 5-10, 13 and 17 stands or falls with that of Claim 1.

Claim 15 is a dependent claim of Claim 1. Claim 15 further defines the apparatus as one where the encryption key is encrypted. The Examiner is of the opinion that the apparatus of Claim 15 is rendered obvious by Warren's disclosure that the encryption keys are distributed in a channel that can be encrypted. A careful reading however of column 16, lines 16-24 and Figure 12 of Warren fails to show that there is any encryption of the encryption key. Rather the data in Warren is encrypted as shown in Figure 17 and it is only the data that is subject of the decryption function 1740 whereas the corresponding encryption key is used, when decoded, to operate the decryption function. For this reason it is submitted that Claim 15 is not rendered obvious by the combination of Warren taken with Rump.

Claim 20 is an independent claim directed to a method for the secure transfer of a data stream from a digital source to a digital data receiver. The method comprises the steps of partitioning the data stream into a plurality of successive data blocks wherein the size of each successive data block is variable based on an average size and based on a randomly generated offset. For each successive data block an encryption key is generated. Each data block is encrypted using the encryption key to provide an encrypted data block. Furthermore, the method includes the step of generating a synchronization index associating the encrypted data block with the encryption key. The Examiner acknowledges that Warren does not disclose having different size data blocks identified by an offset value. However, the Examiner refers to Rump as disclosing a system wherein each block contains a block size index. The Examiner statement in this regard is followed by a conclusion not supported by either references but only by applicant's specification that the single data block is further conditioned by an offset value and that the size of each successive data block is based on an average size and based on a randomly generated offset. These are descriptions from applicant's claims and specification and not from either of these references and is thus an impermissible hindsight reconstruction of the prior art using applicant's specification as a roadmap. For this reason it is submitted that Claim 20 is not rendered obvious by the combination of Warren taken with Rump.

For purposes of this appeal only, the patentability of each of Claims 20-24 and 27 stands or falls with that of Claim 20.

Claim 25 is a dependent claim of Claim 20. Claim 25 further defines the method of Claim 20 with the additional step of encrypting the encryption key. The Examiner is of the opinion that the method of Claim 25 is rendered obvious by Warren's disclosure that the encryption keys may be distributed in a channel that can be encrypted. A careful reading however of column 16, lines 16-24 and Figure 12 of Warren fails to show that there is any encryption of the encryption key. Rather the data in Warren is encrypted as shown in Figure 17 and it is only the data that is subject of the decryption function 1740 whereas the corresponding encryption key is used, once decoded, to operate the decryption function. For this reason it is submitted that Claim 25 is not rendered obvious by the combination of Warren taken with Rump.

Claim 47 is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method includes providing digital motion image data as digital motion image data blocks at least some of which digital motion image data blocks are different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks. In response to an index that provides information identifying a first frame of each digital motion image data block there is generated a corresponding key from a plurality of encryption keys for use in decrypting the respective digital motion image data blocks. At least some of the digital motion image data blocks each represent plural frames of the motion picture. It is respectfully submitted that this combination of steps is not rendered obvious by the combination of Warren taken with Rump. There is no disclosure in Warren of using variability in terms of numbers of frames of motion picture in the image data blocks. While there is description in Warren of having different size blocks once the block size is determined that is fixed for the digital motion picture. This is required because the encryption keys in Warren are sequenced with the respective data blocks, there being no index to identify an encryption key. Rump provides no indication that the data blocks are of plural frames of a motion picture but merely that they are of a size determined by a block size index. For these reasons it is submitted that Claim 47 is not rendered obvious by the combination of Warren taken with Rump.

Claim 52 is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method includes the steps of providing digital motion image data as digital motion image data blocks wherein the data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra-coded and P and B frames are encrypted. The corresponding key from a plurality of encryption keys is generated for use in decrypting the digital motion image data block that is encrypted. It is acknowledged that Warren discloses the providing of MPEG type of compression to the image data blocks. However, there is no description in Warren nor in Rump that the intra-coded and P and B frames are encrypted. For this reason it is submitted that Claim 52 is not rendered obvious by the combination of Warren taken with Rump.

Claim 57 is dependent upon Claim 47 and adds the step that the block boundaries are determined by computation of random offsets. As noted above with regard to the arguments for the patentability of Claim 47 there is no disclosure in Warren of using variability in terms of numbers of frames of motion picture in the image data blocks. While there is description in Warren of having different size blocks, once the block size is determined it is fixed for the digital motion picture. The use of different block boundaries as determined by computation of random offset is also inapplicable to the embodiments of Warren because of the requirement that the encryption key be specifically located relative to the particular block of image data. Rump also fails to suggest the use of random offsets and thus the combination of Warren with Rump would not render obvious the method of Claim 57. For this reason it is submitted that Claim 57 is not rendered obvious by the combination of Warren taken with Rump.

Claim 58 is a dependent claim of Claim 47 and adds the step that indices providing correspondence information relative to encryption keys are provided in the channel separate from a channel providing cipher text of the encrypted data blocks. As noted above with regard to arguments for the patentability of Claim 47, Warren does not rely upon any indices that provide correspondence information relative to encryption keys. It is placement of the encryption key in Warren that establishes its relevance to its corresponding data block. Rump provides no indication that the data blocks are of plural frames of a motion picture but merely that they are of a size determined by a block size index. For these reasons it is submitted that Claim 58 is not rendered obvious by the combination of Warren taken with Rump.

Claim 72 is directed to a method of decryption of a motion picture having a plurality of image frames. The method comprises the steps of providing a plurality of encrypted video image blocks which in combination comprise the motion picture in encrypted form. The encrypted video image blocks each represent information of a plurality of image frames of the motion picture. Each image frame begins at a frame beginning and at least some of the image blocks are sized to encrypt different numbers of image frames. A synchronization field is provided. A key field is provided and comprises a plurality of keys. Each key is suited for decryption of a respective image block. The decryption engine uses the synchronization field and the keys in the key field to create a table or matrix in the memory that maps each key to its respective image block. It is respectfully submitted that this feature is also not disclosed or rendered obvious by the combination of Warren taken with Rump. As noted above Warren is directed to providing an encryption key signal that is fixedly positioned relative to the corresponding encrypted data block. There is no indication or teaching in this reference of a decryption engine that uses the synchronization field and the keys in the key field to create a table or matrix in the memory that maps each key to its respective image block. It is not seen why one of ordinary skill in the art would modify the embodiment of Warren in view of the teaching of Rump absent the suggestions found in applicant's specification. For these reasons it is submitted that Claim 72 is not rendered obvious by the combination of Warren taken with Rump.

Claim 74 is a dependent claim of Claim 73. Claim 74 is directed to in a method for the decryption of an individual image frame of an encrypted motion picture, a method of generating a key for use in decryption of the individual image frame. In this key generating method there is provided an identification of an image frame to be decrypted. There is provided a synchronization index to map a plurality of encryption keys, the keys being suited for use in decrypting respective blocks of image data forming a motion picture. In response to the identification of the image frame and the synchronization index outputting a corresponding key for decrypting of the specific image frame. Claim 74 further includes the feature of defining each image block as being comprised of plural image frames. Thus, in the method of claim 74 a specific image frame may be worked upon such as by an editor without decryption of other image frames within the image block. The Examiner refers to the embodiment of Warren Figure 17 wherein there is provided for the multiplexing of the various signals including image blocks and respective keys. As noted in the specification of Warren the keys are arranged in an orderly arrangement relative to the respective frames so that processing of the key signals and the respective frames by the multiplexer may occur. However, there is no description or teaching in Warren of a synchronization index that maps a plurality of encryption keys so that in response to the identification of the image frame and the synchronization index there is output of the corresponding key for decrypting of the specific image frame. There is furthermore no teaching in Rump of the ability to access one image frame of an image block having plural image frames. For this reason it is submitted that Claim 74 is not rendered obvious by the combination of Warren taken with Rump.

Claim 75 is a dependent claim of claim 74 and additionally includes the feature of defining that at least some of the blocks are of different sizes in terms of number of frames from other blocks. In the embodiments of Warren the blocks of image data are fixed as they are required to be at some relative location with respect to the encryption key. Rump provides for different size blocks but not in terms of numbers of frames. It is submitted therefore that Claim 75 is not rendered obvious by the combination of Warren taken with Rump.

7. Claims 11, 14 are not unpatentable as being obvious in view of Warren taken with Handelman under 35 USC 103. Claims 11 and 14 are dependent upon Claim 1 and further limit this claim with the feature regarding the use of a smart card for the block synchronization data channel and for the key transmission channel, respectively. Claims 11 and 14 are separately patentable.

The Examiner has cited the combination of Warren in view of Handelman as rendering obvious the subject matters of Claims 11 and 14. The Examiner acknowledges that Warren does not disclose using smart cards in the copy management system and notes that the secondary reference, Handelman, discloses a data access system wherein the video data is accessed using a smart card that communicates "seeds, keys and access control algorithms with the video decoder." However, a careful reading of the paragraph of Handeman noted by the Examiner indicates that it is the video data stored in the IC card that access is provided to and that there is no disclosure of the use of the block synchronization data channel that utilizes a smart card (Claim 11). Nor, is their disclosure of a key transmission channel that utilizes a smart card (Claim 14). For these reasons it is submitted that Claims 11 and 14 are each separately patentable over the combination of Warren taken with Handelman.

8. Claim 19 is not unpatentable as being obvious in view of Warren taken with Schneier under 35 USC 103.

Claim 19 is a dependent claim of Claim 18 which is a dependent claim of Claim 1. Claim 1 is directed to a data transfer apparatus for the secure transfer of a plurality of data blocks wherein each data block comprises plural frames of a digital video image. The apparatus comprises an encryption key generator for providing encryption keys wherein a respective encryption key is assigned to each data block. A block synchronization index is provided indicating a correspondence between the encryption key and the data block. A memory stores the encryption keys at a digital data receiver and the digital data receiver includes a decryption engine that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block. Claim 18 further adds that the block synchronization index is computed using a pseudo-random number generator. Claim 19 further defines the pseudo-random number generator as being a linear feedback shift register. According to the Examiner, Warren discloses that the system can use a number of different associations between the encryption keys and the data frames. However, the description of Warren assumes some orderly arrangement of encryption keys is provided so that there is a direct sequence between the encryption keys and the corresponding respective image frames. Thus, in Warren buffering can be used when there is a lack of timely simultaneous presentation of the encryption key and its corresponding image frame or frames. However, there is no disclosure or suggestion in Warren of a synchronization index and further no disclosure of a synchronization index that is computed using a pseudo-random number generator as called for by Claim 19. Still further, there is no disclosure or suggestion in Warren that the pseudo-random number generator be a linear feedback shift register. The Examiner cites the Schneier publication as disclosing that pseudo-random sequences can be generated using a linear feedback shift register. However, there is no suggestion in either reference as to why or how one would use such a generator in the embodiments of Warren which have a fixed placement of encryption keys relative to respective data blocks and not even the need for a synchronization index. The Examiner merely provides a conclusion of obviousness without consideration of the lack of disclosure in Warren of even a synchronization index. The use of the Schneier reference could only have been suggested by impermissible reference to applicant's specification. For this reason it is submitted that Claim 19 is not rendered obvious by the combination of Warren taken with Schneier.

9. Claims 26, 37 are not unpatentable as being obvious in view of Warren taken with Dahan under 35 USC 103. Each of these claims is separately patentable.

Claim 26 is a dependent claim of Claim 20 and therefore includes the subject matter of this claim. Claim 20 is an independent claim directed to a method for the secure transfer of a data stream from a digital source to a digital data receiver. The method comprises the steps of partitioning the data stream into a plurality of successive data blocks wherein the size of each successive data block is variable based on an average size and based on a randomly generated offset. For each successive data block an encryption key is generated. Each data block is encrypted using the encryption key to provide an encrypted data block. Furthermore, the method includes the step of generating a synchronization index associating the encrypted data block with the encryption key. The Examiner acknowledges that Warren does not disclose having different size data blocks identified by an offset value. Claim 26 further defines the method wherein the step of transmitting the encrypted data blocks to the receiver is in a non-sequential order. The Examiner cites Dahan as disclosing that data is written from an optical disk in a non-sequential order. However, there is no disclosure in this combination of the subject matter described above with regard to Claim 20 from which Claim 26 depends. For this reason it is submitted that Claim 20 is not rendered obvious by the combination of Warren taken with Dahan.

Claim 37 is a dependent claim of Claim 36. Claim 36 is an independent claim directed to a method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion image. The method of claim 36 includes the steps of providing a plurality of encryption keys separately from encrypted data blocks and storing the encryption keys in a memory at a digital receiver. An identifier is provided that correlates a mapping algorithm to the plurality of encryption keys and a decryption engine is operated that is responsive to the identifier in the mapping algorithm to generate each key for use in decryption of the respective data block. Claim 37 further defines this method such that a plurality of encryption keys are interleaved in a non-sequential order. In the final rejection the Examiner notes that each data block in Warren contains an encryption key for the frame contained in the next data block "which meets the limitation providing an identifier that correlates a mapping algorithm to said plurality of encryption keys." However, there is no indication of such an identifier that performs this function and the recited step. There is merely the presence of location of the key relative to the data block. There is no identifier that is disclosed that correlates a mapping algorithm to the plurality of encryption keys. Furthermore, the Examiner acknowledges that data is transferred sequentially as opposed to non-sequentially in Warren. However there is no suggestion in Warren that the encryption keys may be interleaved in a non-sequential order as called for in the method of Claim 37. For this reason it is submitted that Claim 36 is not anticipated or rendered obvious by Warren.

10. Claims 42, 45, 46, 50, 53-56 and 76 are not unpatentable as being obvious in view of Warren taken with Chaum under 35 USC 103. Each of the claims are separately patentable.

Claims 42, 45 and 46 are directly or indirectly dependent upon dependent claim 39, which in turn is dependent upon independent claim 36. Claim 36 is an independent claim directed to a method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion image. The method of claim 36 includes the steps of providing a plurality of encryption keys separately from encrypted data blocks and storing the encryption keys into memory into a digital receiver. An identifier is provided that correlates a mapping algorithm to the plurality of encryption keys and a decryption engine is operated that is responsive to the identifier in the mapping algorithm to generate each key for use in decryption of the respective data block. In the final rejection of claim 36 the Examiner notes that each data block in Warren contains an encryption key for the frame contained in the next data block "which meets the limitation providing an identifier that correlates a mapping algorithm to said plurality of encryption keys." However, there is no indication of such an identifier that performs this function and the recited step. There is merely the presence of location of the key relative to the data block. There is no identifier that is disclosed that correlates a mapping algorithm to the plurality of encryption keys. Claim 39 includes the feature that the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame with digital motion image data frame component identification. It is further characterized by the step of generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part. Claim 42 further defines the method of Claim 39 such that decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data on a screen. In Warren there is no teaching of a step of providing a frame or frame component identification that is then used to generate a corresponding key from the plurality of encryption keys for use in decrypting the pertinent data block. There is merely location of corresponding keys with corresponding data blocks but no teaching of generating a corresponding key from the plurality of encryption keys using a frame or frame component identification. Chaum is cited by the Examiner as providing disclosure of a copy protection system that utilizes to video parts in combination at a projector to view the films. However, Chaum is not concerned with encryption nor is there any suggestion made by the Examiner as to why one of ordinary skill in the art would consider this reference other than for the fact that a projector is a known device for projecting a film image. Warren thus fails either taken alone or in combination with Chaum to render obvious the subject matter of Claim 42. For this reason it is submitted that Claim 42 is not rendered obvious by Warren in view of Chaum.

Claim 45 further defines the method of it Claim 39 so that a video frame is defined as comprising pleural color components and only data of one of the color components is encrypted. As noted with regard to arguments pertaining to patentability of Claim 42 immediately above, Warren fails to teach a step of providing a frame or frame component identification that is then used to generate a corresponding key from the plurality of encryption keys for use in decrypting the pertinent data block. There is merely location of corresponding keys with corresponding data blocks but no teaching of generating a corresponding key from the plurality of encryption keys using a frame or frame component identification. Chaum is cited by the Examiner as providing a teaching that frame by frame protection of the film being projected can be performed on a color basis. However, Chaum is not directed to encryption of digital data nor is there any indication as to why one of ordinary skill in the art would consider the type of system in Chaum for modification of the apparatus and method of Warren. For this reason it is submitted that Claim 45 is not rendered obvious by Warren in view of Chaum.

Claim 46 is a dependent claim of Claim 45 and as such is submitted to be patentable if Claim 45 is found to be patentable. Furthermore, Claim 46 further defines the method of Claim 45 by requiring that the color component that is encrypted is represented by a bit depth greater than one and only one bit plane of the color component data is encrypted. There is no indication in the final rejection as to why Claim 46 is deemed to be obvious in view of the combination of Warren taken with Chaum. Subject matter of the method of Claim 46 reduces substantially the amount of encryption needed by having a color component of an image frame represented by plural bits and wherein only certain bits of that color component are encrypted. For this reason it is submitted that Claim 46 is not rendered obvious by Warren in view of Chaum.

Claim 50 is a dependent claim of Claim 47 and as such is submitted to be patentable if Claim 45 is found to be patentable. Claim 47 is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method includes providing digital motion image data as digital motion image data blocks at least some of which digital motion image data blocks are different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks. In response to an index that provides information identifying a first frame of each digital motion image data block there is generated a corresponding key from a plurality of encryption keys for use in decrypting the respective digital motion image data blocks. At least some of the digital motion image data blocks each represent plural frames of the motion picture. There is no disclosure in Warren of using variability in terms of numbers of frames of motion picture in the image data blocks. While there is description in Warren of having different size blocks once the block size is determined that is fixed for the digital motion picture. This is required because the encryption keys in Warren are sequenced with the respective data blocks, there being no index to identify an encryption key. Claim 50 further defines the method of claim 47 by having the decryption of the encrypted data blocks being made in a digital motion image projector which projects images represented by the digital motion image data upon a screen. As noted above Warren fails to render obvious subject matter of Claim 47 from which Claim 50 depends. Chaum merely discloses the use of two projectors for obscuring a part of the movie. There is no disclosure in Chaum regarding the use of encryption keys in accordance with the combination claimed in Claim 50. Neither Warren or Chaum teach the method of providing at least some variability in terms of numbers of frames of the motion picture in the image data blocks and in response to an index providing information identifying a first frame of each digital motion image data block and generating a corresponding key from the plurality of encryption keys for use in decrypting the respective digital motion image data blocks. For these reasons it is submitted that Claim 50 is not rendered obvious by the combination of Warren taken with Chaum.

Claim 53 is an independent claim directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The steps of this claim comprise providing digital motion image data of a digital motion picture as digital motion image data blocks is. The digital motion image data frame comprises plural color components and only data of one of the color components is encrypted. The method of Claim 53 provides for reduced image processing in that only one of the color components is encrypted. The Examiner has recognized that Warren does not disclose that the video signal is encrypted based on color data and thus that Warren does not anticipate or render obvious this claim. Chaum is noted by the Examiner for a general teaching of protection of the frame through manipulation of a particular color within the frame. However, Chaum is not directed to encryption or decryption of the digital data but merely preventing the video capture of a projected image of such a motion picture. It can hardly be said that the disclosure of Chaum would be considered of any use to the routineer with regard to the problem applicant has solved. For these reasons it is submitted that Claim 53 is not rendered obvious by the combination of Warren taken with Chaum.

Claim 54 is a dependent claim of Claim 53 and is patentable if Claim 53 is found to be patentable. Claim 54 further defines the method of Claim 53 by defining that the data of the color component that is encrypted is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of the color component data is encrypted. Thus, there is realized a significant reduction in image processing in that only a part of one of the color components is encrypted. The Examiner has recognized that Warren does not disclose that the video signal is encrypted based on color. Chaum is not directed to encryption or decryption of the digital data but merely preventing the video capture of a projected image of such a motion picture. The combination of Warren taken with Chaum can hardly suggest or render obvious the method of Claim 54 absent impermissible reference to applicant's specification. For these reasons it is submitted that Claim 54 is not rendered obvious by the combination of Warren taken with Chaum.

Claim 55 is a dependent claim of Claim 47. Claim 47 is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method includes providing digital motion image data as digital motion image data blocks at least some of which digital motion image data blocks are different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks. In response to an index that provides information identifying a first frame of each digital motion image data block there is generated a corresponding key from a plurality of encryption keys for use in decrypting the respective digital motion image data blocks. At least some of the digital motion image data blocks each represent plural frames of the motion picture. Claim 55 further defines the method of Claim 47 by reciting that the image data frame comprises plural color components and the data of the color components are encrypted. It is respectfully submitted that this combination of steps is not rendered obvious by the combination of Warren taken with Chaum. There is no disclosure in Warren of using variability in terms of numbers of frames of motion picture in the image data blocks. While there is description in Warren of having different size blocks once the block size is determined that is fixed for the digital motion picture. This is required because the encryption keys in Warren are sequenced with the respective data blocks, there being no index to identify an encryption key. Chaum is not directed to encryption or decryption of the digital data but merely preventing the video capture of a projected image of such a motion picture. The combination of Warren taken with Chaum can hardly be said to render obvious the method of Claim 55. For these reasons it is submitted that Claim 55 is patentable over the combination of Warren taken with Chaum.

Claim 56 is a dependent claim of Claim 55 and is patentable if Claim 55 is found to be patentable. Claim 56 further defines the method of Claim 55 by defining that the data of the color components that are encrypted are each represented by a bit depth greater than one and one or more bit planes but less than all bit planes of the color component data is encrypted. Thus, there is realized a significant reduction in image processing in that only a part of the color components are encrypted. The Examiner has recognized that Warren does not disclose that the video signal is encrypted based on color. Chaum is not directed to encryption or decryption of the digital data but merely preventing the video capture of a projected image of such a motion picture. Thus, the method of Claim 56 cannot be said to be rendered obvious by the combination of Warren taken with Chaum.

Claim 76 is a dependent claim of Claim 73. Claim 73 is directed to in a method for the decryption of an individual image frame of an encrypted motion picture, a method of generating a key for use in decryption of the individual image frame. In this key generating method there is provided an identification of an image frame to be decrypted. There is provided a synchronization index to map a plurality of encryption keys, the keys being suited for use in decrypting respective blocks of image data forming a motion picture. In response to the identification of the image frame and the synchronization index outputting a corresponding key for decrypting of the specific image frame. Claim 76 further defines a method wherein each block comprises a color separation component of an image frame. As noted in the specification of Warren the keys are arranged in an orderly arrangement relative to the respective frames so that processing of the key signals and the respective frames by the multiplexer may occur. However, there is no description or teaching in Warren or Chaum whether combination of a synchronization index that maps a plurality of encryption keys so that in response to the identification of the image frame and the synchronization index there is output of the corresponding key for decrypting of the specific image frame. For this reason it is submitted that Claim 76 is not rendered obvious by the combination of Warren taken with Chaum.

11. Claims 70, 71 are not unpatentable as being obvious in view of Warren taken with Rabowsky under 35 USC 103. Claims 70 and 71 are each separately patentable.

Claims 70 and 71 are each a dependent claim of Claim 66. Claim 66 is an independent claim directed to a data structure providing a keyfile comprising a plurality of respective keys for decryption of respective blocks of frames of the motion picture. The data structure comprises a synchronization field containing synchronization index information operative to link individual keys to respective blocks of video image data. Each block comprises plural frames of the motion picture. A key field representing plural encryption keys are operative for use in decryption of the respective image frames.

Claim 70 further defines the data structure as including a key overhead field containing information including the name of the motion picture.

Claim 71 further defines the data structure of Claim 66 as including a key overhead field containing information containing the name of the theater presenting the motion picture.

As noted above Warren provides correspondence between a key and adds respective image frame or frames through relative location or placement. There is no indication of a data structure providing a keyfile of respective keys with a synchronization field containing synchronization index information to link individual keys to respective blocks of video image data. Rabowsky is cited by the Examiner as disclosing a digital electronic cinema system wherein motion picture files are transmitted with the file name and a specific theater name. The Examiner specifically refers to column 1, line 47-column 2, line 47. While the disclosure of Rabowsky teaches of a headend system and a theater system the latter receiving cinema and data files from the headend system, the cinema file referred to is the movie itself and there is no disclosure that the name of the movie or that the name of the theater is provided in a key overhead field as required by Claims 70 and 71.

It is submitted therefore that the combination of Warren taken with Rabowsky fails to render obvious the subject matters of Claims 70 and 71.

12. Claims 29 and 51 are not unpatentable as being anticipated or obvious in view of the prior art. The final rejection mentions these two claims as being rejected only in the summary and not in the body of the final rejection. Claims 29 and 51 are separately patentable.

Claim 29 is a dependent claim of independent claim 28. Claim 28 is directed to a method for the secure transfer of a digital motion image data stream from a digital data source to a digital data receiver. The method of claim 28 includes the steps of partitioning digital motion image data stream into a plurality of digital motion image data blocks, generating a plurality of encryption keys and generating an encrypted digital motion image data stream by repetition of various recited steps for each of the plurality of digital motion image data blocks. The steps include encrypting each digital motion image data block using a distinct encryption key to create an encrypted video data block. The encrypted data block is stored as part of an encrypted digital motion image data stream. A synchronization index is generated that associates each digital motion image data block with each distinct encryption key providing the encrypted with a digital motion image data stream to the digital data receiver. A synchronization index is provided to the digital data receiver. The encryption keys are stored at the digital data receiver in a memory, and the digital data receiver includes a decryption engine that is responsive to the synchronization index and the decryption engine mapping each key into memory to a respective encrypted data block for use in decryption of the respective data block. Claim 29 further defines the method of Claim 28 as having the step of partitioning digital motion image data stream so that an offset value is used to establish a starting frame for each digital motion image data block and providing different offset value is to establish different sizes of image data blocks. As the Examiner notes Warren discloses a copy management system wherein data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block. In this regard the Examiner refers to Figure 13. The Examiner further refers to Warren's Figure 12 wherein each data block contains an encryption key for the frame contained in the next data block. According to the Examiner this implies and "meets the limitation" of a block synchronization index indicating a correspondence between the encryption key in the single data block. The Examiner is thus apparently of the opinion that the encryption key of Warren is its own index. However, within the disclosure of Warren there is no indication that there is any generation of a synchronization index that associates each said digital motion image data block with each distinct encryption key. There is merely generation of an encryption key that is associated with an image data block. It is submitted that Claim 29 is not anticipated or rendered obvious by Warren taken with any other reference.

Claim 51 is a dependent claim of independent claim 47. Claim 47 is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. The method includes providing digital motion image data as digital motion image data blocks at least some of which digital motion image data blocks are different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks. In response to an index that provides information identifying a first frame of each digital motion image data block there is generated a corresponding key from a plurality of encryption keys for use in decrypting the respective digital motion image data blocks. At least some of the digital motion image data blocks each represent plural frames of the motion picture. Claim 51 further defines the method of Claim 47 wherein the digital motion image data blocks comprises data of the motion picture in compressed form and the entire motion picture is encrypted. It is respectfully submitted that this combination of steps is not rendered obvious by the combination of Warren taken with any of the other references. There is no disclosure in Warren of using variability in terms of numbers of frames of motion picture in the image data blocks. While there is description in Warren of having different size blocks once the block size is determined that is fixed for the digital motion picture. This is required because the encryption keys in Warren are sequenced with the respective data blocks, there being no index to identify an encryption key. There is no indication in the other references of record that the data blocks are of plural frames of a motion picture. For the above reasons it is respectfully submitted that Claim 51 is patentable over the prior art.

Conclusion

For the above reasons, Appellant respectfully requests that the Board of Patent Appeals and Interferences reverse the final rejections by the Examiner and mandate the allowance of Claims 1-3, 5-47, 50-58, and 62-77, which are the only pending claims in the application.

Respectfully submitted,

Attorney for Appellants
Registration No. 29,134

Nelson A. Blish/tmp
Telephone: 585-588-2720
Facsimile: 585-477-4646
Enclosures

If the Examiner is unable to reach the Applicant(s) Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.

Appendix I - Claims on Appeal

1. A data transfer apparatus for secure transfer~~,~~ from a digital data source to a digital data receiver~~,~~ of a plurality of data blocks each data block comprising plural frames of a digital video image, the apparatus comprising:

(a) an encryption key generator for providing encryption keys wherein a respective encryption key is assigned to each data block of the plurality of data blocks and a block synchronization index is provided indicating a correspondence between said encryption key and said data block;

(b) an encryption engine that, for each said data block, produces an encrypted data block using said encryption key from said encryption key generator;

(c) a data transmission channel for delivering said encrypted data block from said encryption engine to the digital data receiver;

(d) a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver;

(e) a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver;

(f) a memory for storing the encryption keys at the digital data receiver; and

(g) said digital data receiver including a decryption engine that is responsive to said synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block.

2. The apparatus of claim 1 wherein said encryption engine and decryption engine are provided with symmetric encryption.

3. The apparatus of claim 1 wherein the size of said single data block is further conditioned by an offset value.

4. (canceled)

5. The apparatus of claim 1 wherein said data transmission channel is a wireless transmission network.

6. The apparatus of claim 1 wherein said data transmission channel utilizes dedicated phone service.

7. The apparatus of claim 1 wherein said data transmission channel utilizes a portable storage medium.

8. The apparatus of claim 1 wherein said data transmission channel utilizes a computer data network.

9. The apparatus of claim 1 wherein said data transmission channel utilizes a local area network.

10. The apparatus of claim 1 wherein said data transmission channel utilizes a wide area network.

11. The apparatus of claim 1 wherein said block synchronization data channel utilizes a smart card.

12. The apparatus of claim 1 wherein said block synchronization index is encrypted.

13. The apparatus of claim 1 wherein said block synchronization data channel utilizes a portable storage medium.

14. The apparatus of claim 1 wherein said key transmission channel utilizes a smart card.

15. The apparatus of claim 1 wherein said encryption key is encrypted.

16. The apparatus of claim 1 wherein said key transmission channel utilizes a portable storage medium.

17. The apparatus of claim 1 wherein said data block is compressed.

18. The apparatus of claim 1 wherein said block synchronization index is computed using a pseudo-random number generator.

19. The apparatus of claim 18 wherein said pseudo-random number generator is a linear feedback shift register.

20. A method for secure transfer of a data stream from a digital data source to a digital data receiver, the method comprising:

(a) partitioning the data stream into a plurality of successive data blocks, wherein the size of each successive data block is variable, based on an average size and based on a randomly generated offset;

(b) generating, for each successive data block, an encryption key;

(c) encrypting each said successive data block using said encryption key to provide an encrypted data block; and

(d) generating a synchronization index associating said encrypted data block with said encryption key.

21. The method of claim 20 wherein the step of providing said encrypted data block comprises the step of recording said encrypted data block onto a recording medium.

22. The method of claim 21 wherein said recording medium uses a magnetic storage technology.

23. The method of claim 21 wherein said recording medium uses an optical storage technology.

24. The method of claim 20 wherein the step of providing said encrypted data block comprises the step of transmitting said encrypted data block to the digital data receiver.

25. The method of claim 20 further comprising the step of encrypting said encryption key.

26. The method of claim 20 further comprising the step of transmitting said encrypted data blocks to said receiver site in non-sequential order.

27. The method of claim 20 wherein said data stream comprises digital motion image data.

28. A method for secure transfer of a digital motion image data stream from a digital data source to a digital data receiver, the method comprising:

(a) partitioning the digital motion image data stream into a plurality of digital motion image data blocks;

(b) generating a plurality of encryption keys;

(c) generating an encrypted digital motion image data stream by a repetition of the following steps for each of said plurality of digital motion image data blocks:

(1) encrypting each said digital motion image data block using a distinct encryption key to create an encrypted video data block;

(2) storing said encrypted data block as part of said encrypted digital motion image data stream;

(d) generating a synchronization index that associates each said digital motion image data block with each said distinct encryption key;

(e) providing said encrypted digital motion image data stream to the digital data receiver;

(f) providing said synchronization index to the digital data receiver;

(g) storing the encryption keys at the digital data receiver in a memory; and

(g) said digital data receiver including a decryption engine that is responsive to said synchronization index and the decryption engine mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block.

29. The method of claim 28 wherein the step of partitioning the digital motion image data stream into a plurality of digital motion image data blocks further comprises:

(a) generating an offset value used to establish a starting frame for each said digital motion image data block and providing different offset values to establish different sizes of image data blocks.

30. The method of claim 28 wherein the step of partitioning the digital motion image data stream into a plurality of data blocks uses a digital motion image frame as a base unit.

31. The method of claim 28 wherein the step of generating a synchronization index further comprises encrypting said synchronization index.

32. The method of claim 28 wherein the step of providing said encrypted motion image data stream to the digital data receiver comprises the step of transmitting said encrypted motion image data stream.

33. The method of claim 28 wherein the step of providing said encrypted motion image data stream to the digital data receiver comprises the step of recording said encrypted motion image data stream onto a storage medium.

34. The method of claim 28 wherein the step of providing said synchronization index to the digital data receiver comprises the step of transmitting said synchronization index.

35. The method of claim 28 wherein the step of providing said synchronization index to the digital data receiver comprises the step of recording said synchronization index onto a storage medium.

36. A method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion the late that image, the method comprising:

(a) providing said plurality of encryption keys separately from said encrypted data blocks and storing the encryption keys in a memory at a digital data receiver;

(b) providing an identifier that correlates a mapping algorithm to said plurality of encryption keys; and

(c) operating a decryption engine that is responsive to said identifier and the mapping algorithm to generate each key for use in decryption of the respective data block.

37. The method of claim 36 wherein said plurality of encryption keys are interleaved in a non-sequential order.

38. The method of claim 36 further comprising the step of padding said plurality of encryption keys using dummy bits.

39. The method of claim 36 and wherein the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part.

40. The method of claim 39 wherein each block is a digital motion image data frame component of a motion picture.

41. The method of claim 39 wherein each block is a digital motion image data frame of a motion picture.

42. The method of claim 39 wherein decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

43. The method of claim 39 wherein the digital motion image data blocks comprise data of a motion picture in compressed form and the entire motion picture is encrypted.

44. The method of claim 39 wherein the digital motion image data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra- coded and P and B frames are encrypted.

45. The method of claim 39 wherein a video frame comprises plural color components and only data of one of the color components is encrypted.

46. The method of claim 45 wherein the color component that is encrypted is represented by a bit depth greater than one and only one bit plane of the color component data is encrypted.

47. A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks at least some of which digital motion image data blocks are of different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks; and

in response to an index providing information identifying a first frame of each digital motion image data block generating a corresponding key from a plurality of encryption keys for use in decrypting a respective digital motion image data block wherein the said at least some digital motion image data blocks each represents plural frames of the motion picture.

48. (canceled)

49. (canceled)

50. The method of claim 47 wherein the decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

51. The method of claim 47 wherein the digital motion image data blocks comprise data of the motion picture in compressed form and the entire motion picture is encrypted.

52. A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks, wherein the digital motion image data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra- coded and P and B frames are encrypted; and

generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted.

53. A method of decrypting encrypted digital motion image data

blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks, wherein a digital motion image data frame comprises plural color components and only data of one of the color components is encrypted; and

generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted.

54. The method of claim 53 wherein the data of the color component that is encrypted is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of the color component data is encrypted.

55. The method of claim 47 wherein a digital motion image data frame comprises plural color components and the data of the color components are encrypted.

56. The method of claim 55 wherein each color component is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of each color component data is encrypted.

57. The method of claim 47 wherein block boundaries are determined by computation of random offsets.

58. The method of claim 47 wherein indices providing correspondence information relative to encryption keys are provided in a channel separate from a channel providing ciphertext of the encrypted data blocks.

59. (canceled)

60. (canceled)

61. (canceled)

62. A data structure for use in providing an encryption key for use in decrypting an image block of encrypted video image, the image block being composed of plural image frames and the encrypted video image being formed of plural image blocks, the data structure comprising:

a component ID field having plural bits mapping information for identifying an image frame of the image block at which a specific encryption key is first used; and

an encryption key field of plural bits forming the encryption key and being operative for use in decrypting the image block.

63. The data structure of claim 62 and including a start component ID field of plural bits that is operative to identify the start of the data structure.

64. A composite data structure having plural component data

structures as defined in claim 63 for providing plural encryption keys for use in decryption of respective plural image blocks of the encrypted video image, each image block being composed of plural image frames and the encrypted video image being formed of plural image blocks, each component data structure comprising:

a component ID field having plural bits mapping information for an image frame of the image block at which a specific encryption key is first used; and

an encryption key field of plural bits forming the encryption key that is operative for use in the decryption of the image block.

65. The composite data structure of claim 64 and including a start component ID field of plural bits that is used to identify the start of the component data structure.

66. A data structure providing a key file comprising a plurality of respective keys for decryption of respective blocks of frames of a motion picture, the data structure comprising:

a synchronization field containing synchronization index information operative to link individual keys to respective blocks of video image data, each block comprising plural frames of the motion picture; and

a key field representing plural encryption keys that are operative for use in the decryption of respective image blocks.

67. The data structure of claim 66 and including a key overhead field having information indicating how keys are arranged in the key field.

68. The data structure of claim 66 and including a key overhead field having information indicating how the blocks of video image data are structured.

69. The data structure of claim 66 and including a key overhead field having information specifying an algorithm used to locate a corresponding key within the key field.

70. The data structure of claim 66 and including a key overhead field containing information including the name of the motion picture.

71. The data structure of claim 66 and including a key overhead field containing information containing the name of a theater presenting the motion picture.

72. A method of decryption of a motion picture having a plurality of image frames comprising:

providing a plurality of encrypted video image blocks of data which in combination comprise the motion picture in encrypted form, the encrypted video image blocks each representing information of a plurality of image frames of the motion picture wherein each image frame begins at a frame beginning and at least some of the image blocks being sized to encrypt different numbers of image frames;

providing a synchronization field;

providing a key field comprising a plurality of keys for use in the decryption of the video image blocks, each key being suited for decryption of a respective image block; and

operating a decryption engine that uses the synchronization field and the keys in the key field to create a table or matrix in a memory that maps each key to its respective image block.

73. In a method for the decryption of an individual image frame of an encrypted motion picture having a plurality of image frames, the method of generating a key for use in the decryption of the individual image frame, the key generating method comprising:

providing an identification of an image frame to be decrypted;

providing a synchronization index to map a plurality of encryption keys, the keys being suited for use in decrypting respective blocks of image data forming a motion picture; and

in response to the identification of the image frame and the synchronization index outputting a corresponding key for decrypting of the specific image frame.

74. The method according to claim 73 and wherein each block comprises plural image frames.

75. The method according to claim 74 and wherein at least some of the blocks are of different sizes in terms of number of frames from other blocks.

76. The method according to claim 73 and each block comprises a color separation component of an image frame.

77. The method according to claim 73 and wherein each key corresponds to only a single image frame so that access to other image frames requires more than one key.

Appendix II - Evidence

none

Appendix III – Related Proceedings

none